Centers for Medicare & Medicaid Services (CMS) Enterprise Development, Security, and Operations (DevSecOps) Effort

Task Order 0003 (47QFLA21K0054-0003)

Continuous Authorization and Verification Engine (batCAVE) Enterprise Platform

Statement of Objectives (SOO)

September 20, 2022

ORGANIZATION:
The CMS is part of the Department of Health and Human Services (HHS) and is the agency with the goal to cover millions of eligible people for enrollment in Medicare, Medicaid, and the Children's Health Insurance Program (CHIP) or in a qualified health plan through the Health Insurance Marketplace. Another goal of the agency is to achieve a high-quality health care system with the aim for better care at lower costs and improved health. In this capacity, CMS is responsible for payment of over $900 billion each year for medical services rendered to the nearly 100 million program beneficiaries and recipients. CMS has a central site in Baltimore and 10 regional offices in major cities throughout the country. CMS contracts with approximately 33 companies to process claims for reimbursement for medical services rendered under the Medicare program and the agency works with all states, the District of Columbia, and the U.S. territories as the focal point for all national program policies and operations related to Medicaid, CHIP, and the Basic Health Program (BHP).

In the administration of these programs, CMS utilizes many assets, including buildings, facilities, communications equipment, computer systems, employees, contractors, public trust, and information. A loss to any one of these assets could affect the goals or the quality of support necessary from CMS to its various customers and stakeholders. Additionally, CMS collects, uses, and stores information that falls into the categories of privacy data, Protected Health Information (PHI), proprietary data, procurement data, inter-agency data, and privileged system information. Access to these types of information is controlled by the Privacy Act of 1974 (as amended), the Computer Security Act of 1987 (as amended), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Federal Information Security Management Act (FISMA) of 2002, as well as many important rules, regulations, policies, and guidelines promulgated by HHS, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). As a result, CMS has a legal and practical responsibility to maintain the confidentiality, integrity, and availability (CIA) of this information.

CMS, like many organizations, faces significant challenges in managing agency risk across its dynamic mission and its large array of networks and information systems. Information assets have become increasingly difficult to protect due to advances in the threat landscape, such as

easy-to-use cyber-attack frameworks, advanced threat actor persistence and technologic attack evolution, data obfuscation, and social engineering such as phishing attacks. These factors have resulted in a critical necessity for utilizing an innovative and forward-thinking implementation of security at the agency. Through innovative advances in the implementation of security, inclusion of security requirements throughout the system and software development life-cycle, and the continuous monitoring and ongoing authorization program, the agency effectively manages risk through an optimal security posture, and thus protects the confidentiality, integrity, and ensures the availability (CIA) of CMS information. Every day CMS has the responsibility to track and report on cyber activity at nearly 50 data centers / sites.

CMS is responsible for collecting, generating, storing, and therefore protecting personal, financial, healthcare, and other sensitive information. Much of this information relates to the healthcare provided to the nation's Medicare and Medicaid beneficiaries and has access restrictions required by legislative and regulatory directives. CMS is responsible for ensuring the CIA of this information, regardless of how it is created, distributed, or stored.

Furthermore, the CMS general support system (GSS) and applications supporting the Affordable Care Act (ACA), Health Insurance Marketplace will be accessed by more than thirty-five million individuals in a given year, and it provides data exchange services to a variety of state governments, issuers, agents / brokers, assistors, and provides backend connections and data transformation services to many federal agencies. Distributed across multiple data centers and supported by a multitude of both contractor and federal personnel, the infrastructure supporting the Health Insurance Marketplace program is a highly complex, dispersed and interdependent environment.

To safeguard the CIA of its information and information systems effectively, CMS has established an enterprise-wide Information Security and Privacy program under the Information Security and Privacy Group (ISPG). The ISPG, charged with protecting CMS data, "provides leadership to CMS in managing information security and privacy risks appropriate for evolving cyber threats." ISPG executes this vision utilizing an innovative approach to provide optimal visibility, situational awareness, resilience and incident response readiness across all CMS FISMA Systems.

The ISPG program is responsible for defining policy, providing security and privacy services, and leading compliance and oversight of the program. This is inclusive of helping application development organizations (ADOs) build and deploy systems quickly and safely. Currently, there is a tremendous amount of overhead placed on ADOs in designing, developing, deploying, and maintaining systems that align with security and privacy requirements.

BACKGROUND:
This task order will derive from and extend work done during the Small Business Innovation Research (SBIR) Phase I contract (FA300219PA158) and SBIR Phase II contract (FA864919CA011) with RevaComm. Detailed SBIR background information is provided in the Indefinite Delivery Indefinite Quantity (IDIQ) Performance Work Statement.

1.0 TASK ORDER OBJECTIVE:

Within CMS, teams frequently build and deploy duplicative technology solutions to solve problems, fueling more complexity across the IT ecosystem and increasing the burden on end users and development teams. In order for the Continuous Authorization and Verification Engine (batCAVE) platform to successfully integrate into existing IT environments and security policy across CMS there are a variety of enterprise integrations that are necessary, abstracting some of this complexity away. This task order will enable the platform to make use of existing identity management and orchestration solutions without excessive and costly rebuilding efforts. This task order is also focused on building capabilities to satisfy Executive Order 14028 requirements around zero trust, logging, and software integrity verification within the batCAVE platform.

2.0 SCOPE:

The scope of this project covers expanded enterprise software integration, systems development, and data engineering efforts for the CMS batCAVE platform and supporting products, including platform instrumentation, continuous integration and deployment pipelines, and continuous authorization support. This project also covers developer enablement and enterprise integration support for development teams looking to re-architect and migrate their FISMA systems or vendor commercial off the shelf (COTs) products to the platform.

3.0 TASK/TECHNICAL REQUIREMENTS:

This effort will conduct and/or develop plans for research, development, and applications to meet the requirements for technologies identified within the following areas:

3.1. Product Team Organization (Overall Management Objectives) (IDIQ 2.3.1)

The contractor shall, in coordination with the Government, assemble and manage product delivery teams for each value stream of the platform to include product management support, human centered design, and core engineering resources. The contractor shall participate in daily standups during non-holiday business days. Value streams centered around the functional areas of the batCAVE platform and delivery teams to include but not limited to:

- Security data lake engineering
- Enterprise identity management Application Programming Interface (API) and integrations
- Zero Trust (ZT) and single sign on authentication (SSO)

The contractor shall provide product management and human centered design support to support key cybersecurity leadership that intersect with and support the batCAVE platform-as-a-service and cloud program. Specific examples include:

- Security data lake
- Software bill of materials and software supply chain risk management
- System and cloud governance and compliance

3.2 Optional Objective 1 – Enterprise API Services Development (Severable) (IDIQ 2.4)

The contractor shall, in coordination with the Government, create an enterprise API service that accomplishes four key objectives aligned with the batCAVE platform:

3.2.1 Modernize Identity and Access Management (IAM)

- Create an IAM API service that acts as a shim between legacy systems and authentication services with Okta to eventually move the enterprise to Okta as the single source of truth where multi-factor authentication (MFA) (using hardware enabled authentication devices such as yubikey) and ZT can be enabled.
- To achieve this a middleware application shall be created that pulls IAM data from internal legacy CMS systems and feeds it through an API to Okta, initially creating two sources of truths that should act as a mirror and then eventually phase the legacy authentication and role-based access controls out.

3.2.2 Share Application Data

- As CMS moves to fully enabled web applications, an API shall be created to start to warehouse data in various applications. For example, all cyber scheduling app data could be housed in same datastore, and other applications (like CFACTS or Aolytix) could use this data. Alternatively, cyber scheduling could use data from security tooling such as Nucleus, Axonius, or CFACTs that will help to add context.

3.2.3 Create Extensible Middleware to Feed Security Data Lake

- Create an API service that takes logging and monitoring data from any type of app or logging and monitoring service (the CMS deems relevant) and feeds it to snowflake, in a normalized manner. The requirement would be for any application teams to send the requested data through the API service so CMS stays agnostic of logging/monitoring tools.

3.2.4 Automation

- Leverage the above API objections to automation provisioning and access to various systems and tools. From here, the contractor shall create an extensible & programmatic way to not only allow access to IAM, but how teams automate access to their tools through ZT, SSO, etc.

3.3 Objective 2 – Security Data Lake Engineering (Severable) (IDIQ 2.4)

The contractor shall, in coordination with the Government, develop a security-focused data lake to support petabyte-scale log aggregation for application telemetry, security operations data, and security program data in relation to the batCAVE platform, ISPG mission, and applications running within the CMS Cloud. This shall include:

- Building data governance and data access rules into data lake platform to inform authorization decisions made in alignment to CMS security policy.
- Support for a security data lake shall also include the development and operation of extraction, load, and transform (ETL) pipelines to ingest selective data sets into the security data lake.

- Deployment and operation of solutions to ingest, normalize, and aggregate data necessary for the cybersecurity mission at CMS

3.4 Objective 3 – Onboarding and Platform Helpdesk (Severable) (IDIQ 2.4)
The contractor shall, in coordination with the Government, support application development organizations (ADOs) in their migration to and consumption of the batCAVE platform. This shall be done using a high-touch embedded engineering model to support cross-training, technical work required to migrate, superior customer support of technical issues, and act as a communication interface to the broader batCAVE platform engineering team(s).

3.5 Optional - Objective 4 – Zero Trust Model and Single Sign On Automation (Severable) (IDIQ 2.4)
The contractor shall, in coordination with the Government, help to establish a Zero Trust Architecture (ZTA) as a pilot for batCAVE and integrate it with Yubikey (or a similar hardware security product) to achieve a hardware device MFA process throughout the batCAVE environment. This shall include:

- Completed architect decision records (ADR) for ZTA, zero trust tooling, and MFA hardware devices with consideration on how it will play within the larger enterprise.
- Integrate the ZTA with existing CMS SOO/Identity and Access Management tools (IAM) (Okta or Azure Active Directory).
- Integrate zero trust and MFA with all batCAVE tooling to include, but not limited to logging, monitoring, support, pipeline tools, and gitlab.
- Write documentation and user guides for setting up the batCAVE/CMS accounts to leverage zero trust and MFA.
- Manage control mapping for the ZTA, ZT, and MFA to achieve future Authority to Operate (ATO).

3.6 Optional - Objective 5 – Platform Engineering Scale (Severable) (IDIQ 2.4)
The contractor shall, in coordination with the Government, add mapping of controls to the newly released Acceptable Risk Safeguards (ARS) 5.0 for batCAVE and expand upon initial work to focus on CMS Cloud Integration as a product owner.

Integrations points, include but is not limited to:

- Transition of testing-as-a-service (TaaS) and cloud continuous integration and continuous delivery (CI/CD) to batCAVE
- Map batCAVE and cybersecurity scheduling for controls to ARS 5.0 for Security Impact Analysis (SIA) and ATO purposes.
- Help to create sherpa model for onboarding of teams on to batCAVE that is supported that with platform-as-a-service (PaaS) educational tools.
- Integrate with site reliability engineering (SRE) and operations stacks for enterprise availability and monitoring.
- Cost estimator for batCAVE and integration with onboarding.

3.7 Objective 6 – Enterprise Cost and Scale (Severable) (IDIQ 2.4)

The contractor shall, in coordination with the Government, develop capabilities to capture and forecast costs related to infrastructure, time, and data management. This work shall include capturing, modeling, and analyzing data related to cost, tagging of resources, and creating traceability for ownership. This work should inform procurement spend optimization efforts within the Office of Information Technology (OIT) and the CMS Cloud Program.

3.8 Objective 7 - Open-Source Environment Contribution (Severable) (IDIQ 2.4)

The contractor shall, in coordination with the Government, contribute enhancements back to the BATcave Platform, Big Bang, and related software ecosystem as appropriate. As appropriate, the contractor shall facilitate the publication of additional open-source system components and code in support of CMS and the BATcave platform.

3.9. Optional - Objective 8 - Governance, Risk, and Compliance Tooling Modernization (Severable) (IDIQ 2.4)

The contractor shall, in coordination with the Government, deploy, optimize, and maintain a modernized governance, risk, and compliance (GRC) solution to support CMS compliance needs. This work shall support:

- Complete ADR to select a new enterprise GRC tool
- Ensure that it complies with ARS 5.0 and various NIST frameworks and that it supports an appropriate inheretence model
- Ensure that compliance artifacts can managed and verified through native Open Security Controls Assessment Language (OSCAL) formats
- Deploy tooling within batCAVE infrastructure and that it can be secured per CMS specification
- Ensure that it can be integrated with SSO and ZTA
- Ensure that multiple application development organizations (ADOs) can be supported while still providing CMS an enterprise view of GRC posture
- Ensure that an API is available so integration with other OIT and ISPG technologies can be accomplished to cut out duplicative work being required of other OIT or ADO
- Data sharing via API integrations with other OIT and ISPG technologies to cut out duplicative work being required of OIT or ADO team members

As necessary, this work may require migration of compliance data out of existing legacy GRC tooling.

3.10 Optional - Objective 9 – Operations (Engineering) and Site Reliability Engineering (SRE) Support (Severable) (IDIQ 2.4)

The contractor shall, in coordination with the Government, provide Operations (Engineering) and Site Reliability Engineering (SRE) engineering resources to engage with and support key CMS initiatives such as Open Enrollment. This work shall support:

- Supplementation of the existing scope of Operations (Engineering) and SRE with cloud engineering resources to improve cloud operations and processes
- Optimization of the onboarding process and incorporation of SRE identified recommendations to overall process improvement that represents
- Support for critical systems monitoring and availability across high-priority CMS operational activities (i.e. Medicare Open Enrollment, Marketplace Open Enrollment, Production migration & Severity incidents)
- Increased knowledge transfer across the CMS Cloud Program (including PaaS, Infrastructure as a Service (IaaS), security, etc.) and working closely/supporting
- Deploying & integrating tools and processes to support improvements in system uptime, performance, visibility, and security operations

4.0 DELIVERABLES

All software developed under this task order shall be delivered in accordance with IDIQ PWS paragraph 4. The contractor shall identify, within the proposal, any restrictions on the type of rights to be provided with software and hardware delivered but not developed on this task order with full disclosure of any dependencies upon third party software/hardware. The software shall be installed and demonstrated in a client named facility, and/or other facilities specified by the Government client Technical Point of Contact (TPOC). Additionally, the following deliverables are required for this task order.

Deliverable Title	Delivery Due Date	Delivery To
Project kickoff meeting	No later than (NLT) 10 days after the award of this task.	GSA's web-based procurement system (i.e., Assisted Services Shared Information System (ASSIST) Collaboration), Client Representative (CR) and Alternate Client Representative (ACR)
Monthly Status, Labor Hour, and Expenditure Report (MSR)	No later than (NLT) 15th calendar day of the month following the reporting period.	Contractor format unless specified. Submitted simultaneously with the Invoice in ASSIST
Invoice with supporting documentation and MSR	NLT 15th calendar day of the month following the reporting period.	ASSIST

Program Management Reviews	Every three months. Meeting minutes are due NLT 2 business days following the meeting.	Contractor format unless specified; with delivery to ASSIST Collaboration, CR, and ACR
System Documentation	Due date – as agreed upon with the government technical lead. Usable documented information provided in an accurate, clear, complete, consistent manner, and contains the appropriate level of detail. This document should be a living document	ASSIST Collaboration, CMS owned project website in coordination with CR/ACR
Software and Platform Delivery	Due date – as agreed upon with the government technical lead. Data deliverables are produced using prescribed formats, software tools, and software versions as agreed to by the Government. All deliverables meet professional standards for technical writing and the requirements set forth in the contract. Deliverables should also include a memo outlining received/acceptance documentation. Provide required software and tooling to support Task delivery.	CMS owned Github repositories and cloud environments in coordination with CR/ACR
Project Planning and Management	The contractor shall develop a living document that maintains project plans 100% compliant with federal governing regulations, policies, directives, guidance and industry practice.	ASSIST Collaboration and CR/ACR

	100% of project plans shall include the identification of applicable responsibilities, timelines, deliverables, risks, milestones and other elements as required. 100% of plan schedules and activities shall be coordinated with all required participants. All issues impacting project schedules shall be communicated to government staff within one business day after determination of impact. Project plans shall be updated and delivered weekly.	
Sprint Reviews	Review at the end of Each Sprint and submit a post sprint newsletter. Following the completion of each delivery sprint a sprint review will be conducted to ensure delivery artifacts satisfy customer and partner requirements and to solicit early feedback. Deliverables should also include a memo outlining received/acceptance documentation.	Contractor format unless specified; Review to be performed with project delivery team lead.
Briefings	Upon request by Government; Draft (due 1 week post completion) and Final Briefing to be presented to Government 2 days after the draft briefing	Contractor format unless specified; ASSIST Collaboration and delivery to CR and ACR

	Meeting minutes are due NLT 2 business days following the Briefing.	

5.0 ADDITIONAL PERFORMANCE REQUIREMENTS

5.1 Location of Work. The primary place of performance for this task order will be at the contractor's facility or remotely at the contractor's discretion and must be within the United States inclusive of Hawaii and Alaska.

5.2 Travel. There is no travel expected or required for this task order. All work shall be performed within the CONUS at the discretion of the Contractor.

6.0 SECURITY REQUIREMENTS

In accordance with Homeland Security Presidential Directive (HSPD)-12, contractor access to HHS-controlled facilities, information technology systems, or sensitive data, all Contractor staff of this acquisition must be cleared at a minimum of Public Trust 6 (PT6) background investigation level.

7.0 RECORDS MANAGEMENT

All data and deliverables are the property of CMS and are required to be maintained in accordance with the HHS/Office of the Chief Information Officer (OCIO)'s policy on records management. This policy is available at:

http://www.hhs.gov/ocio/policy/2007-0004.001.html. All reports created shall be submitted to CMS via email or a CMS provided portal.

8.0 PERIOD OF PERFORMANCE

The period of performance for this task order will include a 12-month base period, four 12-month option periods. The effort shall include schedules, milestones, and approaches to complete this task. The contractor shall provide a schedule, within the Project Plan deliverable, that encompasses 60 months of technical effort.

9.0 SECTION 508 - ACCESSIBILITY OF INFORMATION and COMMUNICATIONS (ICT) TECHNOLOGY

Refer to section 9.4 of the IDIQ PWS.

10.0 FEDERAL INFORMATION SECURITY MANAGEMENT ACT(FISMA) of 2002

CMS collects, uses, and stores information that falls into the categories of privacy data, Protected Health Information (PHI), proprietary data, procurement data, inter-agency data, and privileged

system information. Access to these types of information is controlled by the Privacy Act of 1974 (as amended), the Computer Security Act of 1987 (as amended), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the FISMA of 2002. As a result, CMS and the Contractors that perform work on our behalf have a legal and practical responsibility to maintain the confidentiality, integrity, and availability (CIA) of this information.

FISMA is applicable to the proposed acquisition in as much as the Contractor's responsibility will include protecting federal information and federal information systems by conducting cybersecurity operations and assisting in the development of IT security policies. Rather than developing an IT security test plan and performing IT assessments, the contractor shall review in such assessments and conduct of security assessments. The Contractor shall comply with relevant HHS policies to include HHS OCIO Policy for Enterprise Architecture. A copy of this policy is available at: http://www.hhs.gov/ocio/policy/index.html.

11.0 HHS Enterprise Performance Life Cycle (EPLC)

All IT systems development or enhancement tasks supported by the contractor shall follow the HHS Enterprise Performance Life Cycle (EPLC) framework and methodology. Information about EPLC policy and framework is available at http://www.hhs.gov/ocio/policy/2008-0004.001.html and http://www.hhs.gov/ocio/eplc-lifecycle-framework.pdf.

12.0 GOVERNMENT FURNISHED PROPERTY

CMS will not be supplying government furnished property (GFP); contractors will be accessing CMS systems utilizing virtual desktop infrastructure (VDI.)

13.0 OTHER DIRECT COSTS

The Government may require the contractor to purchase materials and equipment and ODCs, to include hardware, software, and related supplies critical and related to the services being acquired under the contract/order. Such requirements will be identified at the time the contract/order is issued or may be identified during the course of a contract/order by the Government or the contractor. If the contractor initiates a purchase within the scope of the contract/order and the prime contractor has an approved purchasing system, the contractor shall submit to the GSA COR a Request to Initiate Purchase (RIP). If the prime contractor is to lose or does not have an approved purchasing system, the contractor shall submit to the CO a Consent to Purchase (CTP). The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not make any purchases without an approved RIP from the GSA COR or an approved CTP from the CO.)

14.0 SOO ATTACHMENTS

- NIST 800-53 Rev. 5 (DOI) Link: Assessing Security and Privacy Controls in Information Systems and Organizations (nist.gov)
- Cloud.cms.gov website
- Draft Service Delivery Summary (SDS)

- Draft Quality Assurance Surveillance Plan (QASP)
- Request to Initiate Purchase (RIP)
- Consent to Purchase (CTP)